Department of Homeland Security Daily Open Source Infrastructure Report for 13 March 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports Delta Air Lines' terminal at LaGuardia Airport was evacuated for about two hours on Friday, March 10, due to an alert, which turned out to be a false alarm, triggered when a man's shoes set off a security screening device meant to detect explosives. (See item 10)
- The Department of Homeland Security reports during a two−week enforcement action that culminated on March 9, federal agents from the U.S. Immigration and Customs Enforcement arrested 375 gang members and associates in 23 states under Operation Community Shield. (See item 15)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 10, MarketWatch* — **BP set to seal leaking Alaska pipeline.** BP Plc. said Friday, March 10 it hoped to soon wrap up repairs to a leaking pipeline on Alaska's giant Prudhoe oil field that has already spilled over 200,000 gallons of crude, one of the biggest spills ever seen on the state's North Slope. In a joint statement with the federal Environmental Protection Agency and state officials, BP said an early assessment puts the volume of oil spilled at 201,000 to 267,000 gallons of crude, or roughly 6,000 barrels. So far, a clean−up crew of 60

has recovered about 52,920 gallons of liquids, though that includes snow and ice scooped up in the process. BP operators discovered a quarter−inch hole in the 34−inch diameter, above−ground pipeline on Thursday, March 2, prompting the company to curtail output on the field by about 100,000 barrels of crude oil a day. Prudhoe Bay, the biggest oil field in the U.S., typically pumps about 470,000 barrels a day. Oil from the field is carried via the Trans−Alaska pipeline over the Brooks Mountain Range to a tanker terminal in Valdez on Alaska's Prince William Sound.
Source: http://www.marketwatch.com/News/Story/Story.aspx?guid=%7BDC3B7830%2DE553%2D40F2%2D94BD%2D288E25A96F81%7D&dist=rss&siteid =mktw

2. *March 10, Associated Press* — **Plant's reactor shuts down after turbine failure.** The reactor at a nuclear power plant on Lake Ontario automatically shut down overnight due to a turbine failure. Constellation Energy operates the Nine Mile Point Unit 2 plant at Scriba, NY. Plant operators say the loss of vacuum in a steam condenser system caused the turbine to trip. Constellation spokesperson Jill Lyon says the reactor safely shut down, and the faulty component has been replaced with a redundant condenser system.
Source: http://www.wrgb.com/engine.pl?station=wrgb&id=3784&template=breakout_regional_story.shtml&dateformat=%25M+%25e,%25Y

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *March 09, U.S. Department of Defense* — **Pace details DoD's supplemental funding needs.** Reconstructing and replacing equipment, force protection, defeating improvised explosive devices, and "resetting" the Army are among necessities that Department of Defense's (DoD) emergency supplemental budget request would fund, Marine General Peter Pace said Thursday, March 9. The $91 billion bill would fund military operations in the war on terror and Hurricane Katrina relief, Pace, the chairman of the Joint Chiefs of Staff, told the Senate Appropriations Committee. Reconstituting equipment is a priority for troops in Afghanistan and Iraq, which the supplemental asks for $10.4 billion to cover, the chairman said. "It goes to replenish Humvees and trucks and helicopters and Bradley fighting vehicles and all the things that we have been using, getting damaged, wearing out in the prosecution of this war," Pace said. Leaders are not simply replacing equipment one for one. Pace said the government is buying and resetting for the force of the future. The military will buy V−22 Ospreys, for example, instead of helicopters and seven−ton trucks rather than the current five ton models. The supplemental requests a further $2.6 billion for troop force protection.
Source: http://www.defenselink.mil/news/Mar2006/20060309_4441.html

4. *March 09, Government Computer News* — **Air Force looking beyond Network Centric Solutions program.** Although it awarded the five−year contract in late 2004, the Air Force is

already thinking beyond its $9 billion Network Centric Solutions program because it falls short of meeting the service's enterprise−wide needs, according to an Air Force procurement official. Matthew Benavides, director of acquisitions and commodities at the Air Force's Operations and Sustainment Systems Group near Montgomery, AL, said the concern "is that Netcents already has a shelf life, and we're starting to think about how we can replace it," Benavides said. The Air Force will likely hold an industry day and release a draft request for proposals for IT Services in May.
Source: http://www.gcn.com/online/vol1_no1/40083−1.html

[Return to top]

Banking and Finance Sector

5. *March 10, Deseret Morning News (UT)* — **Credit union members report fraudulent e−mails in phishing scam.** Two odd e−mails arrived in the in−boxes of hundreds of members of Utah Community Credit Union (UCCU) on Thursday, March 9, part of an intricate scam to trick them into revealing their credit card numbers, bank account numbers, and passwords. Brigham Young University employees were among the targets of the attempted phishing scam. The attack Thursday was the first on UCCU. Mountain America Credit Union also was targeted recently. The fraudulent email messages claimed to be reminders of unusual activity on customer accounts, and the e−mails urged customers to click on a link in the messages and confirm personal records on a Website. UCCU chief information officer Ken Gibby said the two fake Websites were tracked to servers in China and Japan. UCCU officials contacted the FBI. Mountain America has 89,000 members who used the credit union's Online Branch banking service. UCCU has about 45,000 active users of its Personal Branch online service. Notable characteristics of the fraudulent e−mail include the date of the unusual activity was listed as "06.03.2006," the European style of denoting March 6, 2006, and a Web address with the Chinese domain name www.playersclub.cn.
Source: http://deseretnews.com/dn/view/0,1249,635190747,00.html

6. *March 10, Agence France−Presse* — **Taiwan cracks largest money laundering gang.** Taiwanese authorities have arrested 22 men and confiscated nearly U.S. $625 million after cracking the island's largest money laundering operation, prosecutors said. Lu Po−hsien, suspected mastermind of the money−laundering ring, was arrested Thursday, March 9, at his home where police discovered cash and cashier's checks, said Hsiao Yu−cheng, head of the Chiayi prosecutor's office in southern Taiwan. The other 21 suspected members of the ring were nabbed in 17 raids all over the island, Hsiao said. Lu allegedly engaged in massive money laundering in several locations including China, Hong Kong, the Philippines and Singapore through phony companies he set up in Taiwan and the Cayman Islands. The ring is suspected of laundering millions in the last six years, and faces a minimum prison term of seven years for violating banking, anti−money laundering, anti−fraud and anti−gambling laws, Hsiao said.
Source: http://au.biz.yahoo.com/060310/33/l7t1.html

7. *March 09, Security Park (UK)* — **Police confidential information leaked by virus−infected computer.** According to the Japanese press, information about 1,500 individuals related to police investigations over a three−year period was leaked from a virus−infected computer belonging to an Okayama Police investigator. The data is said to have been distributed to users

of the Winny peer−to−peer file−sharing system. Winny is the most popular file−sharing network in Japan, with over a quarter of a million users. According to the report, the leak occured because the policeman was storing data about investigations on his personal computer. The PC was infected with an unnamed computer virus which is said to have enabled Winny users across Japan to access the sensitive information. "It's bad enough when an individual has data stolen from them by a virus, but a police force being the victim is a real cause for concern," said Graham Cluley, senior technology consultant at Sophos.
Source: http://www.securitypark.co.uk/article.asp?articleid=25042&Ca tegoryID=1

8. *March 09, Oregonian* — **Check inquiry identifies 21 suspects.** A year−long investigation by the Portland, OR, Police Bureau into a counterfeit check cashing ring has led to a 312−count indictment of 21 suspects, authorities said Wednesday, March 8. The ringleader, Gerald Thomas Greenwood, assisted by Tammie Louise Wright, admitted to creating 1,600 counterfeit checks, and they coordinated the distribution of checks, police said. The couple and the others in the ring cashed $150,000 in checks between May and October of 2004, said Melissa Chureau, a Multnomah County deputy district attorney. Evidence shows that about 20 local and out−of−state businesses, ranging from a nursery and lumber company to a Clackamas County school district, and between five and 10 individuals lost more than $58,000 as a result, Chureau said. Actual losses are closer to more than $500,000, she said. The suspects met at parties and through mutual acquaintances and often used methamphetamine, police said. U.S. Bank fraud investigators joined the Multnomah County district attorney's office, the Police Bureau's east precinct neighborhood response team, and east precinct patrol officers in the investigation. A grand jury indicted the 21 suspects February 28, Chureau said. The charges include identity theft, forgery, theft, conspiracy, computer crime, and drug possession, Chureau said.
Source: http://www.oregonlive.com/news/oregonian/index.ssf?/base/new s/1141878330216230.xml&coll=7

9. *March 09, CBC News (Canada)* — **Canadian police break up major identity theft scam.** Police in Ottowa, Canada, have put a stop to a major identity theft scam that preyed on more than 120 victims across Canada and allegedly racked up more than $500,000 worth of charges on bogus credit cards. After searching a house on Tuesday, March 7, police found 60 credit cards, social insurance cards, and drivers licenses issued in the names of victims. Victims identified on the cards come from Ontario and Quebec, and as far away as Nova Scotia and Alberta. Police allege the couple used online employment ads to lure victims to send resumes, then sent a letter to the job seeker promising a high−paying position. The letter requested candidates to send a $20 administration fee and fill out an application form. The form asked for personal information such as a social insurance number, driver's license, full name, and address. Police believe the accused began the scam as early as 2002. Through the years, it has operated under a variety of fake company names, including Microtel Media, Logistic Telecom, Idcor and Pastel Media. Police estimate the accused ran up $500,000 in charges on the credit cards.
Source: http://www.cbc.ca/ottawa/story/ot−theft20060309.html?ref=rss

[Return to top]

Transportation and Border Security Sector

10.

March 11, Reuters — **LaGuardia terminal reopens after scare.** The Delta Air Lines' terminal at New York's LaGuardia Airport was evacuated for about two hours on Friday, March 10, because of a security scare, officials said. A spokesperson from the Transportation Security Administration (TSA) said departing flights had resumed at about 5 p.m. EST after the alert turned out to be a false alarm triggered when a man's shoes set off a security screening device meant to detect explosives. The TSA said the man walked away from the checkpoint apparently unaware that his shoes had set off an alarm. The man was not located but the alert proved to be a false alarm. McCauley said the screening device sometimes is triggered by substances other than explosives, including traces of fertilizer that can be found on the bottom of shoes.
Source: http://news.airwise.com/story/view/1142053104.html

11. *March 11, United Press International* — **Newark airport security shaken up.** The Transportation Security Administration (TSA) has removed two of the top supervisors at Newark Liberty International Airport. Security operations at Newark in New Jersey have been a problem for several years, with screeners failing to find concealed weapons in tests. In the shakeup, Mark Hatfield Jr., who was sent to Newark from TSA headquarters, will be federal security director.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20060311−07430 7−2419r

12. *March 10, CNN* — **Mini microchips avoid lost luggage.** RFID −− radio frequency identification −− is currently being tested at several airports to keep better track of luggage. Unlike traditional bar codes, RFID chips don't have to be in direct view of a scanner to be read, only within a broadcast range of about 15 feet. Currently, around 15 percent of bar codes printed onto the labels placed on checked−in luggage are not properly read automatically, meaning either an expensive manual check or −− worse for travelers −− a suitcase heading down the wrong chute and onto the wrong plane. According to estimates from the International Air Transport Association (IATA), the global aviation industry body that is helping to co−ordinate the introduction of the new technology, around 99 percent of RFID tags are read automatically. "There are several trials under way around the world at the moment," said Andrew Price, who is managing RFID technology for the IATA. Despite the improved efficiency, shifting to RFID requires a considerable investment. Although the scanners are relatively cheap, around $1,000 each, every bag needs a tag, currently costing just over 21 cents each, as against the virtually negligible price for a printed bar code label.
Source: http://www.cnn.com/2006/TRAVEL/03/07/RFID/index.html

13. *March 10, Associated Press* — **Japanese airliner has cracked windshield on way to Guam.** A Japanese airliner carrying 447 people from Tokyo to Guam had to return to Japan shortly after takeoff Friday, March 10, when a cockpit window cracked. JAL Flight 941 landed safely at Narita International Airport near Tokyo. The incident marked the latest in a string of safety issues for Japan Airlines, JAL's parent company. JAL's image has been tarnished by a series of safety problems since early 2005. In Friday's case, cracks fanned out like a spider's web to cover the left cockpit window about 30 minutes after takeover while the airliner, with 22 crew and 425 passengers, was at an altitude of 39,000 feet, JAL spokesperson Atsushi Abe said. Japan Airlines is investigating the cause of the cracks, he said.
Source: http://www.usatoday.com/travel/flights/2006−03−10−cracked−wi ndshield_x.htm

14.

March 10, Government Accountability Office — **GAO−06−259: Immigration Benefits: Additional Controls and a Sanctions Strategy Could Enhance DHS's Ability to Control Benefit Fraud (Report).** In 2002, the Government Accountability Office (GAO) reported that immigration benefit fraud was pervasive and significant and the approach to controlling it was fragmented. Experts believe that individuals ineligible for these benefits, including terrorists and criminals, could use fraudulent means to enter or remain in the U.S. GAO was asked to evaluate U.S. Citizenship and Immigration Service's (USCIS) anti−fraud efforts. This report addresses the questions: (1) What do available data and information indicate regarding the nature and extent of fraud? (2) What actions has USCIS taken to improve its ability to detect fraud? (3) What actions does the Department of Homeland Security (DHS) take to sanction those who commit fraud? To enhance the Department of Security's (DHS) efforts to control benefit fraud, GAO recommends that USCIS implement additional internal controls and best practices to strengthen its fraud control environment and that DHS develop a strategy for implementing a sanctions program that includes a mechanism for assessing their effectiveness and that considers the costs and benefits of sanctions, including their deterrence value. DHS generally agreed with four of the six recommendations but cited actions indicating it has addressed GAO's other two recommendations. GAO believes that additional actions are needed.
Highlights: http://www.gao.gov/highlights/d06259high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−259

15. *March 10, Department of Homeland Security* — **ICE arrests gang members and associates in enforcement action.** During a two−week enforcement action that culminated on Thursday, March 9, federal agents from the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE) arrested 375 gang members and associates in 23 states in a joint effort with law enforcement agencies nationwide. The arrests are the latest under the auspices of "Operation Community Shield," a comprehensive initiative launched by ICE roughly one year ago to disrupt and dismantle transnational, violent street gangs. Operation Community Shield represents the first time the federal government has used immigration and customs authorities in a combined, national campaign against criminal street gangs in the United States. More than 260 of the 375 individuals arrested in the latest action have past criminal records, most of them violent. ICE agents arrested 73 of the individuals on new criminal charges ranging from drug and firearms violations to charges of re−entering the country after deportation. The rest have been accused of administrative immigration violations and placed into deportation proceedings. Operation Community Shield was launched in February 2005 after a threat assessment by ICE field offices identified MS−13 as one of the largest and most violent street gangs in the country.
Secretary Chertoff press conference on Operation Community Shield:
http://www.dhs.gov/dhspublic/display?content=5478
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0878.xml

16. *March 09, Reuters* — **New transit machines could detect explosives.** Hoping to thwart a potential attack on American subways similar to the London public transit bombings last July, the U.S government is testing ticketing machines that would detect traces of explosives on the fingers of someone buying a subway ticket. The machines are equipped to detect traces of explosives on the fingertips of ticket buyers. If they work as intended, the machines could have the potential to give police an early warning that a bomber may be entering the transit system.

Last July three bombs exploded on London underground trains and a fourth rocked a public bus, killing 56 people, including the four bombers, and injuring 700. Since then, security and transit officials in large U.S. cities such as New York have been seeking ways to better protect their public transportation from such an attack. The automatic ticket vendor, which is under review by the Department of Homeland Security, has been selected for a transit pilot program in Baltimore, MD, coming up in the next six weeks, said spokesperson Jae Lande.
Source: http://news.yahoo.com/s/nm/20060309/tc_nm/security_transport_dc_5

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *March 11, U.S. Department of Agriculture* — **Inconclusive bovine spongiform encephalopathy test results.** "Last night we received an inconclusive test result on a rapid bovine spongiform encephalopathy (BSE) test from an animal sampled as part our enhanced BSE surveillance program," said Chief Veterinary Medical Officer John Clifford of the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service. "USDA is conducting further tests at the National Veterinary Services Laboratories (NVSL) in Ames, IA, using an immunohistochemistry test. In addition, USDA's Agricultural Research Service, will also conduct a Western blot test. The results of those tests will be released as soon as they have all been completed, within the next four to seven days. "This inconclusive result does not mean we have found a new case of BSE. Inconclusive results are a normal component of most screening tests, which are designed to be extremely sensitive so they will detect any sample that could possibly be positive. In addition, this animal did not enter the human food chain nor the animal feed chain."
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/03/0080.xml

18. *March 11, Washington Post* — **Chesapeake's rockfish overrun by disease.** A wasting disease that kills rockfish and can cause a severe skin infection in humans has spread to nearly three−quarters of the rockfish in the Chesapeake Bay, cradle of the mid−Atlantic's most popular game fish. The mycobacteriosis epidemic could carry profound implications for the rockfish, also known as striped bass. The fish fuel a $300 million industry in Maryland and Virginia, but because the bacteria kill slowly, effects on the stock are only now emerging. Researchers know that the Chesapeake, where most rockfish spawn, also breeds the bacterium and is the epicenter of the disease. Yet they don't know how or why it appeared, whether it will spread to other species or if the infection it causes is always fatal. In humans who touch the fish, the microbe can cause a skin infection known as fish handler's disease, which is not life−threatening but can lead to arthritis−like joint problems if untreated.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03/10/AR2006031002416.html

19. *March 10, Animal and Plant Health Inspection Service* — **New York Trees to be treated against Asian longhorned beetle.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (aPHIS) will treat approximately 51,100 trees susceptible to the Asian longhorned beetle (ALB) in New York City this spring. These treatments are part of the ALB cooperative eradication program's effort to prevent further infestation of this invasive insect pest and reduce beetle populations. APHIS will treat trees in portions of the 132−square mile quarantine area in New York with the insecticide imidacloprid, which has yielded positive results in past treatments. Program officials will begin the treatment schedule with approximately 11,282 trees in Manhattan starting in mid−March. Treatment to approximately 22,900 trees in Brooklyn will follow starting in early April. By mid−April, the treatment of 17,000 trees in Queens will begin. The larvae of the ALB bore into healthy hardwood trees and feed on living tree tissue and heartwood. Later, throughout the summer, adult beetles emerge from exit holes and briefly feed on the leaves and small twigs of host trees. To fight this destructive invader, agriculture officials have removed and destroyed more than 6,000 trees infested with ALB in and around New York City and Long Island since the insect was found in Brooklyn in 1996.
Source: http://www.aphis.usda.gov/newsroom/content/2006/03/alb06tre. shtml

20. *March 09, Animal and Plant Health Inspection Service* — **Implementation of animal identification numbers under National Animal Identification System announced.** The U.S. Department of Agriculture (USDA) is announcing plans to begin allocating animal identification numbers (AINs) to tag manufacturers and approving visual identification tags for use under the National Animal Identification System (NAIS), paving the way for distribution of these tags to producers. The initial implementation of AINs focuses on cattle. The use of AINs with other types of identification devices (e.g., implants) used in other species will be considered as the NAIS species working groups finalize their recommendations for utilizing the AIN. USDA also is providing an option to use supplemental identification methods or technologies (e.g., radio−frequency and biometrics) that enhance the utility of AIN tags. Supplemental identification methods or technologies are optional and may vary among species. To ensure compatibility and uniformity is achieved in the national program, USDA's Animal and Plant Health Inspection Service will establish technology standards, when applicable, along with performance requirements for these technologies.
NAIS information: http://animalid.aphis.usda.gov/nais/index.shtml
Source: http://www.aphis.usda.gov/newsroom/content/2006/03/aintag_vs .shtml

21. *March 09, Agence France−Presse* — **European Union experts test three sheep for mad cow disease.** European health experts have identified three cases of a brain disorder in sheep and will conduct tests to see whether it is mad cow disease, the European Commission said. The experts said tests on two sheep from France and one from Cyprus had uncovered an "unusual molecular profile" that must be further investigated, the European Union executive said in a statement. No case of mad cow, or bovine spongiform encephalopathy (BSE), has ever been found in sheep although scientists have long thought it would be possible for them to contract it. The first case of BSE in a goat was found last year.
Source: http://news.yahoo.com/s/afp/20060309/hl_afp/euhealthdiseasea nimal_060309174206;_ylt=AnffBU4.9KPvszUX7vywGDGJOrgF;_ylu=X3 oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Food Sector

22. *March 10, Food Safety and Inspection Service* — **Chicken entrees recalled.** Serenade Foods Division, a Milford, IN, firm, is voluntarily recalling approximately 75,800 pounds of frozen stuffed chicken entrees that may be unhealthful and therefore unfit for food, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Friday, March 10. The raw chicken entrees, because of their frozen state, labeling, and cooked appearance, may have caused consumers to believe these raw products are pre−cooked and therefore consumers may not be cooking these products to a safe temperature. Because of these characteristics, consumers may not be following cooking instructions. The products were contaminated with Salmonella Enteritidis that causes human illness. Illnesses have been linked directly to these products through case history of the patients and through microbiological testing of both the products and affected consumers. The problem was discovered by a Minnesota Department of Health and Minnesota Department of Agriculture investigation into reported foodborne illnesses related to these products. The Minnesota Department of Health contacted FSIS after receiving positive Salmonella Enteritidis test results of the products. The frozen stuffed chicken entrees were distributed to retail establishments nationwide. Source: http://www.fsis.usda.gov/News_&_Events/Recall_009_2006_Relea se/index.asp

[Return to top]

Water Sector

23. *March 10, Philadelphia Inquirer* — **U.S. accuses workers of dumping sewage.** Federal authorities charged two Bristol, PA, Township employees with felony violations of the Clean Water Act Thursday, March 9, on allegations that they dumped untreated sewage into the Delaware River. The sludge polluted a section of the river with fecal coliform bacteria. There is no indication that drinking water was affected, the Environmental Protection Agency (EPA) says. The charges were lodged nearly nine months after EPA investigators carted boxes of files from the Bristol Township Wastewater Treatment Plant and authorities subpoenaed workers. The U.S. Attorney's Office said the plant superintendent and an operator deliberately discharged thousands of gallons of sewage into the river at least twice between August and September 2004. They also are charged with disconnecting alarms that would have signaled a lack of bacteria−killing chlorine in the discharge, and with falsifying test results by disinfecting samples before sending them to EPA−authorized laboratories from 1997 to June 2005. Source: http://www.philly.com/mld/inquirer/news/local/states/pennsyl vania/counties/bucks_county/14061611.htm

[Return to top]

Public Health Sector

24.

March 12, Reuters — **Cameroon becomes fourth African state with bird flu.** Cameroon on Sunday, March 12, became the fourth country in Africa to report an outbreak of bird flu after the disease was found in domestic poultry in its northernmost province. "The first case of bird flu has been detected in the Far North province," the government said in a statement read on state radio. It did not specify what strain of the disease had been found. But France's RFI radio said tests at the Pasteur Institute in Paris showed it was the highly pathogenic H5N1 avian influenza strain, which has already been confirmed in domestic poultry flocks in Nigeria, Niger, and Egypt. Cameroon's Far North province borders to the west with Nigeria, where Africa's first outbreak of H5N1 bird flu was confirmed on February 8. The disease has now spread to 11 states in Nigeria, Africa's most populous nation, from the far north to the far south.
Source: http://za.today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006-03-12T123659Z_01_ALL232855_RTRIDST_0_OZATP-BIRDFLU-CAMEROON-20060312.XML

25. *March 12, New York Times* — **Hospitals short on ventilators if bird flu hits.** No one knows whether an avian flu virus that is racing around the world might mutate into a strain that could cause a human pandemic, or whether such a pandemic would cause widespread illness in the U.S. But if it did, public health experts and officials agree on one thing: the nation's hospitals would not have enough ventilators, the machines that pump oxygen into sick patients' lungs. Right now, there are 105,000 ventilators, and even during a regular flu season, about 100,000 are in use. In a worst-case human pandemic, according to the national preparedness plan issued by President Bush in November, the country would need as many as 742,500. A typical hospital ventilator costs $30,000, and hospitals, operating on thin profit margins, say they cannot afford to buy and store hundreds of units that may never be used. Cheaper alternatives can be deployed in a crisis, but doctors say they are grossly inadequate to deal with a flu pandemic. In a recent emergency drill, said John L. Hick, at the Mayo Medical School in Minnesota, the 27 hospitals in his area could come up with only 16 extra ventilators when faced with a hypothetical outbreak of 400 cases of pneumonic plague.
Source: http://www.nytimes.com/2006/03/12/national/12vent.html?ex=1142744400&en=1eba01708436b246&ei=5065&partner=MYWAY

26. *March 10, Associated Press* — **Panel recommends development of polio drugs.** Development of one or more drugs to treat polio was recommended Thursday, March 9, to provide protection in any outbreaks of the disease that might occur after vaccination programs are ended. A worldwide vaccination effort cut the number of polio cases from more than 350,000 in 1988 to just 784 in 2003, and the World Health Organization (WHO) hopes to reduce the number to zero in the next few years. Once the disease is eliminated it will be difficult to maintain the effort to vaccinate people, and WHO plans to stop using the current vaccine three years after the last case is reported. But there still might be outbreaks of polio, especially as the number of unvaccinated people grows, prompting a committee of the National Research Council to recommend developing antiviral medications to fight polio. The National Research Council is an arm of the National Academy of Sciences, an independent organization chartered by Congress to advise the government on scientific matters.
Source: http://www.cbsnews.com/stories/2006/03/10/ap/health/mainD8G8 V8F07.shtml

27. *March 10, Reuters* — **Global measles deaths fall by nearly half.** Worldwide measles deaths had dropped 48 percent in six years as immunization efforts reached more children in

sub−Saharan Africa, the United Nations said on Friday, March 10. A safe, cheap and effective measles vaccine has been available since the 1960s, but the highly infectious disease is still a major killer of children in developing countries. About 410,000 children under the age of five died from measles in 2004.
Source: http://news.yahoo.com/s/nm/20060310/hl_nm/measles_who_dc;_ylt=AvDZ2Bv.MbpKdWKBn8pknvoQ.3QA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

28. *March 10, Agence France−Presse* — **World Health Organization to create anti−bird flu taskforce.** The World Health Organization (WHO) said that it will create a new taskforce to help tackle outbreaks of bird flu and contain a potential influenza pandemic among humans. Keiji Fukuda, the coordinator of the WHO's global influenza program, told reporters that training of what is initially expected to be a hundred−strong pool of experts may begin as early as the summer. "We need people from a wide variety of backgrounds," Fukuda said, including epidemiologists, laboratory specialists, plus experts in logistics, ethics, and communications. The planned role of the taskforce would include helping countries to probe outbreaks of bird flu, as well as getting in place measures to slow and stop the spread of the disease.
Source: http://news.yahoo.com/s/afp/20060310/hl_afp/healthfluwho_060310185202;_ylt=AqD3KJtdy6Z.rPA88L4oFP.JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

29. *March 10, Los Angeles Times* — **Mystery illness in Chechnya.** Zareta Chimiyeva was at her desk when she smelled "a bad smell," and started feeling ill. She rushed out of the classroom but made it only as far as the stairs. When Zareta woke up in a hospital, it took three adults to hold her down. She wasn't alone. Thirteen other girls were in nearby hospital rooms, also saying they were unable to breathe. The next day, 23 students and seven teachers in a neighboring village fell ill with similar symptoms. About the same time, four−dozen children in two towns a little farther away also began clutching their throats, screaming and convulsing. They have yet to get better. The outbreak began December 16, and doctors and parents say the children are still suffering fits day and night. The list of victims has grown to 93, including several teachers and janitors. After chemical and radiation tests, authorities with the government announced that the culprit was not poison, but a form of mass hysteria. Yet with public health officials at a loss to explain why after months of treatment the children are only getting worse, parents are not ready to accept the official diagnosis.
Source: http://www.latimes.com/news/nationworld/world/la−fg−sickness10mar10,1,1993993.story?coll=la−headlines−world

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *March 10, Facts (TX)* — **Local industries and emergency response teams in Texas simulate oil spill disaster.** Huddled around computers, maps and paperwork, more than 100 representatives from Lake Jackson, TX, industries and emergency response teams worked together Thursday, March 9, to combat a simulated oil spill in Freeport Harbor during a disaster drill. At the Lake Jackson Civic Center, Texas General Land Office and U.S. Coast Guard officers worked alongside port officials and Community Awareness Emergency Response teams from 17 local businesses, police departments and fire departments. The event was an opportunity for the emergency groups to meet each other and work through situations they could encounter, said Rock Lowery, manager of health, safety and the environment at ConocoPhillips Sweeny refinery, which sponsored the drill. The event was designed to get people out of their comfort zones and force them to deal with a major problem before a serious event occurs, Lowery said.
Source: http://thefacts.com/story.lasso?ewcd=82114ed517687a7c

31. *March 10, Norman Transcript (OK)* — **Oklahoma obtains five Regional Hazardous Materials Response Units.** Oklahoma cities of Norman and Moore were presented with a 43−foot−long, specially equipped truck Thursday, March 9, designed to assist emergency workers in responding to natural disasters, hazardous spills or terrorist attacks. In all, five Regional Hazardous Materials Response Units were delivered to Moore/Norman, Tulsa, Oklahoma City, Lawton, and Claremore. The vehicles cost $446,000 each and carry about $300,000 in equipment, including computerized command centers, satellite communications systems, infrared substance monitors, splash suits and breathing masks. Each is strategically placed along the Interstate−44 corridor to enable quick statewide response to incidents.
Source: http://www.normantranscript.com/localnews/local_story_069010235?keyword=secondarystory

32. *March 10, Government Accountability Office* — **GAO−06−338: Telecommunications: States' Collection and Use of Funds for Wireless Enhanced 911 Services (Report).** "Enhanced 911" (E911) service refers to the capability of public safety answering points to automatically receive an emergency caller's location information. An industry association estimates that nearly 82 million 911 calls are placed each year by callers using mobile phones. Wireless E911 technology provides emergency responders with the location and callback number of a person calling 911 from a mobile phone. The ENHANCE 911 Act of 2004 called for the Government Accountability Office (GAO) to study state and local use of funds collected for the purpose of wireless E911 implementation. GAO is reporting on (1) the progress made in implementing wireless E911 services throughout the country, (2) the states and localities that have established taxes, fees, or charges for wireless E911 implementation, and (3) the states or localities that have used funds collected for the purposes of wireless E911 for unrelated purposes. To address these issues, GAO surveyed state−level E911 contacts on the collection and use of E911 funds. Of the 51 state E911 contacts (including the District of Columbia) who were asked to participate in the survey, GAO received 44 responses.
Highlights: http://www.gao.gov/highlights/d06338high.pdf
Survey: http://www.gao.gov/special.pubs/gao−06−400sp/toc.html
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−338

33. *March 09, Daily Reflector (NC)* — **National Guardsmen team with East Carolina University to drill for possible disaster response.** National Guard soldiers, some in

camouflage, others wearing protective jumpsuits, joined Greenville, NC's, East Carolina University (ECU) officials Wednesday, March 8, for a training exercise designed to prepare local emergency responders to handle potential disasters. Creating a scenario where an early morning explosion left two men "sick," the National Guard's Greenville−based 42nd Civil Support Team worked with ECU's police department, environmental health and safety group, public information office and state public health officials to limit human exposure to the fallout. The mission of the exercise was to identify the hazard, retrieve a sample and take all steps necessary to secure the area believed to be contaminated by radiation. ECU officials said their goal was to meet responders and become familiar with procedures needed in the event of an actual disaster.
Source: http://www.reflector.com/news/content/news/stories/2006/03/09/20060309GDRdrill.html?cxtype=rss&cxsvc=7&cxcat=9

34. *March 09, Engineering News−Record* — **Goal is to craft a coordinated and interdependent regional response to a large−scale earthquake in Pacific Northwest.** An unprecedented public−private partnership in the Pacific Northwest is tackling the region's most unsettling scenario −− a magnitude 9.0 earthquake along the Pacific Ocean's 800−mile Cascadia subduction zone that would affect Vancouver, Canada, to San Francisco, CA. The goal is to craft a coordinated and interdependent disaster response plan from myriad self−contained plans. The action plan, intended as a model for regional disaster response regardless of the trigger, will be shared with other areas. The first visible step toward the goal was a March 1−2 "infrastructure interdependencies" workshop in Bellevue, WA, called Blue Cascades III (BC III): Managing Extreme Disasters. The 328 participants represented government emergency management and transportation agencies, utilities, hospitals, schools, law enforcement, fire departments, telecommunications firms and other businesses. The intention of BC III is to raise awareness and gain knowledge of gaps in disaster preparedness planning and management. Other objectives include highlighting laws that might impede restoration or recovery efforts. And participants hope to examine problems that arise from artificial jurisdictional boundaries. An April 27 meeting is set to develop an action plan, including future projects and field drills.
Source: http://enr.ecnext.com/coms2/summary_0271−25563_ITM

35. *March 07, Tribune−Star (IN)* — **Indiana Regional Response Team Task Force 7 members study up on weapons of mass destruction at workshop.** Tuesday, March 7, a weapons of mass destruction workshop for emergency medical personnel was conducted in Terre Haute, IN. About 25 members of the Indiana Regional Response Team Task Force 7 attended the three−day training in the Landsbaum Center for Health Education. The workshop included exercises in the signs and symptoms of chemical, biological, radiological, nuclear and explosive terrorism. The program uses a human patient simulator, which allows participants hands−on practice dealing with patients who exhibit signs of chemical and biological agent exposure. Since 2001, about 40,000 people in Indiana have been trained in the program, said Joseph A. Bell, chief of the terrorism training section at the Indiana Homeland Security Institute.
Source: http://www.tribstar.com/news/local_story_066220552.html

[Return to top]

Information Technology and Telecommunications Sector

36. *March 09, SecuriTeam* — **Eighteen ways to escalate privileges in Zone Labs ZoneAlarm Security Suite.** A locally exploitable security vulnerability in Zone Labs ZoneAlarm Security Suite allows normal users to elevate their privileges. Analysis: Instead of using the full path to the DLL during the load process only the name of the DLL is used. This causes several instances of Windows PATH trolling where Windows tries to locate the DLL in the directories listed in its PATH environment variable on behalf of the vsmon.exe process. This PATH trolling is what makes the vsmon.exe process vulnerable to several privilege escalation techniques. Vulnerable product: Zone Labs ZoneAlarm Security Suite build 6.1.744.000. Patches/Workarounds: The vendor was notified several times but there was no response. Source: http://www.securiteam.com/windowsntfocus/5IP012KI0K.html

37. *March 09, CNET News* — **Gartner forecasts slowing PC market.** PC growth looks set to ease in 2006 as desktop demand shrinks in mature economies, Gartner said Thursday, March 9. Worldwide PC growth is expected to be 10.7 percent in 2006, as compared to growth of 15.5 percent in 2005.
Source: http://news.com.com/2061−10792_3−6048176.html

38. *March 08, Hackers Center* — **Symantec Ghost multiple vulnerabilities.** Three vulnerabilities have been reported in Symantec Ghost, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information, modify certain data, and potentially gain escalated privileges. Analysis: Default administrator login ID and password left behind during installation can be used by local users to modify or delete stored administrative tasks. This can be exploited to modify tasks to run arbitrary code on the local system. Insecure permissions in the shared memory sections within the Sybase SQLAnywhere database used by Symantec Ghost can potentially be exploited to gain access to, and to modify information stored in the database. A boundary error in the login dialog box of dbisqlc.exe, which is installed as a part of the SQLAnywhere package, can cause a buffer overflow. This can potentially be exploited to gain access to information stored in the database that is not normally accessible. Vulnerable: Symantec Ghost 8.x; Symantec Ghost Solution Suite 1.x.
Solution: Update to Symantec Ghost 8.3 that is shipped as a part of Symantec Ghost Solutions Suite 1.1.
Source: http://www.hackerscenter.com/archive/view.asp?id=23418

39. *March 08, Security Tracker* — **Linux kernel dm−crypt fails to clear key storage.** A vulnerability was reported in dm−crypt in the Linux kernel. A local user can obtain information about cryptographic keys. Analysis: The dm−crypt component does not properly clear the crypt_config structure before freeing the structure, which may allow a local user to obtain cryptographic keys. Versions affected: 2.6.15 and prior versions.
Solution: The vendor has issued a fixed version (2.6.16−rc1).
Source: http://securitytracker.com/alerts/2006/Mar/1015740.html

40. *March 08, Security Tracker* — **Xerox WorkCenter Pro multiple PostScript processing errors let remote users deny service.** Several vulnerabilities were reported in Xerox WorkCenter Pro and Xerox CopyCenter. A remote user can cause denial−of−service conditions. Analysis: A remote user can send a specially crafted PostScript file to the target printer to trigger a buffer overflow in the PostScript file interpreter code and cause denial−of−service conditions on the target system. In addition, a remote user can send a

specially crafted PostScript file to traverse the directory and cause denial−of−service conditions on the target system. A remote user can also send a specially crafted PostScript file designed to expose TCP/IP ports to cause denial−of−service conditions on the target system. Additionally, a remote user can trigger a memory error in the Web server code to cause denial−of−service conditions. An unspecified vulnerability exists in the ESS/Network Controller. A user may be able to disconnect power to cause Immediate Image Overwrite to fail without indication.
Vulnerable products: The WorkCenter Pro 65, 75, and 90 models and the CopyCenter C65, C75, and C90 models are affected.
Solution: The vendor has issued a fixed version (1.001.02.074). This security bulletin supersedes Security Bulletin XRX04−008. The vendor's advisory is available at:
http://www.xerox.com/downloads/usa/en/c/cert_XRX06_002.pdf
Source: http://securitytracker.com/alerts/2006/Mar/1015738.html

41. *March 07, Business Weekly (UK)* — **Computer viruses a growing concern for UK companies.** Infection by viruses was the biggest single cause of the worst security incidents for UK companies in the past two years, accounting for roughly half of them, a new survey shows. Two−fifths of these were described as having a serious impact on the business, according to findings from the 2006 Department of Trade and Industry's biennial Information Security Breaches Survey, conducted by a consortium led by PricewaterhouseCoopers. The research showed that virus infections were more likely to have caused service interruption than other incidents. In addition, a quarter of UK businesses are not protecting themselves against the threat caused by spyware. The full results of the ninth, biennial survey will be published at the Infosecurity Europe exhibition and conference in London, April 25−27.
Survey: http://www.ukmediacentre.pwc.com/Content/Detail.asp?ReleaseID=1817&NewsAreaID=2
Source: http://www.businessweekly.co.uk/news/view_article.asp?articl e_id=10229

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document:
http://www.us−cert.gov/reading_room/securing_browser/#sg eneral

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 25 (smtp), 445 (microsoft−ds), 139 (netbios−ssn), 32774 (sometimes−rpc11), 42011 (−−−), 32459 (−−−), 49200 (−−−), 18235 (−−−), 12106 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

42. *March 10, Associated Press* — **FBI: No credible terror threat for college basketball tournaments, but vigilance urged.** The FBI said Friday, March 20, there is no specific, credible threat of a terror attack aimed at college basketball arenas or other sports stadiums, but acknowledged alerting law enforcement to a recent Internet posting discussing such attacks. The FBI and Department of Homeland Security distributed an intelligence bulletin Friday to state and local law enforcement nationwide describing the online threat against sporting venues, said Special Agent Richard Kolko, an FBI spokesperson in Washington. With conference tournaments taking place this weekend, and the NCAA tournament scheduled to begin next week, the bulletin was sent "out of an abundance of caution," Kolko said. The online message described a potential attack in some detail, calling it an efficient way to kill thousands of people using suicide bombers armed with explosives hidden beneath their winter clothing, said a federal law enforcement official who read the bulletin.
Source: http://sportsillustrated.cnn.com/2006/basketball/ncaa/wires/03/10/2060.ap.bkc.ncaa.terror.threat.2nd.ld.writethru.0380/

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer